


Matthew J. Harmon  
Minneapolis, MN • 612-987-0115 • [resume@mjh.email](mailto:resume@mjh.email)  
 [0000-0003-1632-8927](https://orcid.org/0000-0003-1632-8927) • [matthewjharmon.com](http://matthewjharmon.com)

- Cyber Incident Responder, Teacher, Infrastructure Architect, Mentor, Author
- Computer Science (Cyber Security) Instructor and Course Author (Off. Sec, Def. Sec, Linux)
- SANS Instructor for SEC 401 (Security Essentials), SEC 504 (Incident Response), 464 (Ret.)

## EXPERIENCE

CONFIDENTIAL / Information Security, Global  
(2020 / 04) – Present

- Lead incident response operations across a global organization and improving team processes.
- Threat hunter digesting, researching, writing, and implementing efficient cross-platform hunts.
- Built and deployed hyper-accountable, non-attributable infrastructure for high-risk global operations creating a multi-cloud solution enabling new business opportunities and reducing engagement risk.
- Lift organizational units security posture while minimizing downtime.

IT RISK LIMITED / Co-Founder and Principal Consultant, Minneapolis  
(2010 / 08) – (2019 / 12)

- Built a security consulting firm that performed risk assessments, audits, and red team activities.
- Led remediation assistance and treatments for customer pre-audit findings while improving value.
- Led the building of client security operations teams, augmented with our staff as needed.
- Built a secondary "small and medium business" division, bringing cost-effective enterprise security measures to small a medium-sized organizations by partnering with local not-for-profits.

Saint Paul College /

(2017) – (2018) Part-Time Faculty (Computer Science Professor), Saint Paul

(2014) – (2016) Advisory Committee for Cyber Security Associates of Applied Science Program

Teaching Computer Science and Cyber Security Assoc. in Applied Science as a Primary Instructor:

- CSCI 2461 70 & 71, Computer Networking 3 – Linux,
- CSCI 2480 40, Network Security & Penetration Prevention,
- CSCI 2482 40, Security Incident Handling, Response, and Disaster Recovery,
- CSCI 2484 40, Ethical Hacking & Countermeasures.

SANS INSTITUTE / Instructor (Part Time / Independent Contractor), North America  
(2008) – (2021)

Instructor teaching Full Day, Week-Long & Local Mentor Format:

- SANS SEC 401, "Security Essentials" (GSEC),
- SANS SEC 464, "Hacker Detection for Systems Administrators,
- SANS SEC 504, "Incident Handling and Hacking Techniques" (GCIH).

Q.E.D. SYSTEMS / CTO, Worldwide

(1998 / 08) - (2010 / 07)

- Built technology services and implemented control measures for a remote enterprise.
- Led and coordinated the development of standards within ANSI, ISO, and the ITU.:
  - Participant in ISO JTC 1 / SC 27 (IT Security), Participant in SC 31 / WG 7 (Security),
  - Liaison Officer from ISO/TC 122 to ISO/TC 247 (Fraud countermeasures and controls),
  - Chair of ISO/IEC JTC 1/SC 31/US AIDC 1/TG 7 "Security" (Security for Item Management).

THE MITRE CORPORATION / INFOSEC Engineer/Scientist, D.C.

(2001 / 03) – (2003 / 02)

- Intrusion detection and threat analysis, exploit and vulnerability analysis:
  - We discovered CVE 2001-0144, Snort 1 RuleID sig 1324 for SSH1 CRC32 /bin/sh vulnerability.
  - National Infrastructure Protection Center Author, CVE Editor.
- Our team created the "MIDAS" intrusion detection and threat analysis system used internally in MITREs Computer Emergency Response Team and deployed worldwide.

## VOLUNTEER

CYBERSECURITY SUMMIT / Advisory Board, Central Region, US  
(07/2013) - (2020)

Board member, technology lead, received visionary leadership award "The Morries."

SECURITY B-SIDES MSP / Advisory Board, Minneapolis / Saint Paul  
(11/2013) - (08/2017)

Event organizer and volunteer providing leadership and technology services for the cyber security education event.

(ISC)<sup>2</sup> TWIN CITIES CHAPTER / Co-Founder & President, Minnesota  
(03/2012) - (11/2014)

Elected chapter president, and provided monthly education to cybersecurity professionals.

## EDUCATION

- GIAC (Global Information Assurance Certification):
  - Security Essentials (GSEC #19748)
  - Incident Handler (GCIH #20483)
  - Intrusion Analyst (GCIA #9570)
- (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP #333906)
- Aviatix Certified Engineer (ACE) Multi-Cloud Networking Associate (ACE #2021-10689)
- Gaming Commission Class E License (2015)

## SKILLS

- Virtualization / Cloud, Platforms: AWS, GCP, OCI, and VPS providers, Artifact and Packet Analysis, and Log Parsing (Splunk, Numpy/Pandas, Log Explorer), Cloud and Metal Forensics
- Linux: Reverse (and forward) Engineering, Platform Building, CI/CD pipeline, Network Engineering and Monitoring, Configuration Orchestration, Velociraptor, GRR
- Windows: Defender for Enterprise, Tanium, sysinternals
- Management: Conflict resolution, de-escalation, mentoring, event/task organization, team building, cost control by efficient processes and open source software, up-skilling resources

## PUBLISHED

- Contributor to CVE 2001-0144 and Snort 1 RuleID sig 1324 (2001)
- Published in ISO Focus+ "Plugging RFID Security Gaps" (04/2010)
- Published in CSO Outlook "Taking control of IT Operations through the 20 CSC" (06/2015)
- Contributor to ISO/IEC 24791-6, SC 31, Software system infrastructure - Part 6: Security
- Contributor to ISO/IEC TR24729-4, Information technology - Radio frequency identification for item management - Implementation guidelines - Part 4: Tag data security
- Contributor to ISO/IEC 21450-{1,2,4} IEEE 1451.{1,2,4}, Information technology - Smart transducer interface for sensors and actuators - Common functions, communication

## MEDIA

- Interviewed by WCCO for a TV spot about Security B-Sides MSP 2014 (2014)
- Interviewed for Tech Pro (by the Tech Republic) report on Risk Assessments (2014)
- Interviewed for Tech Pro (by the Tech Republic) article on Penetration Testing (2015)
- Interviewed by KSTP for a television report on ATM Skimming (05/2015)
- An expert panel with Minneapolis / Saint Paul Business Journal on Cyber Security (10/2017)
- Interviewed by KSTP for television reports on Breaches (2016-2018)